RSAC 2025 Conference

Many Voices.
One Community.

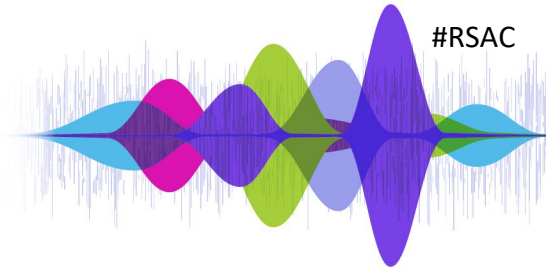
SESSION ID: ANI-R06

Hello It's Me, I'm the User: DBIR Insights on the Use of Stolen Credentials

Philippe Langlois

Lead Data Scientist
Verizon Business Group

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

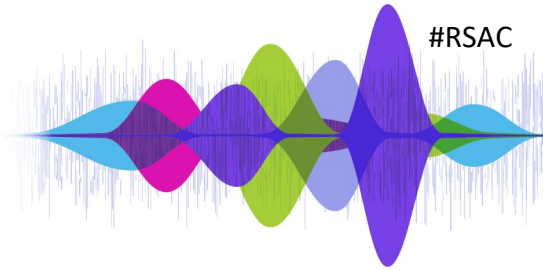
The views expressed during this presentation are the personal views of the speaker and are not necessarily the views of any US Government agency; and not an endorsement or recommendation of any specific policy position.

© 2025 Verizon or its affiliates. The Verizon logo and other trademarks are proprietary. All rights reserved.

Outline

- Data Breach Investigations Review (DBIR) View of Stolen Credentials
- Infostealer Ecosystem
  - What are logs?
  - What marketplaces?
  - What are the buyers?
- What can you do

A comprehensive look at data security patterns



18

years of the Verizon Data Breach Report

22,052

incidents reviewed in our 2025 report

139

victim countries identified

12,195

data breaches analyzed in our 2025 report

Credentials and Ways In

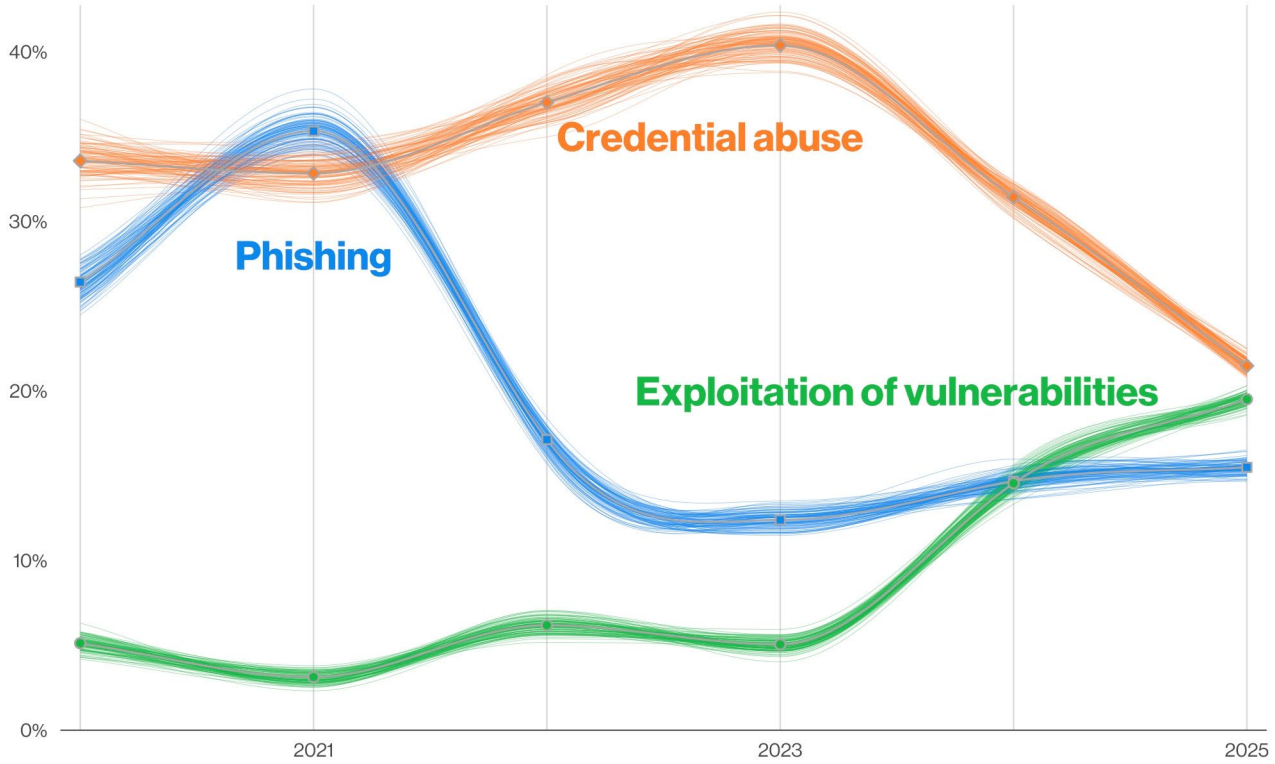
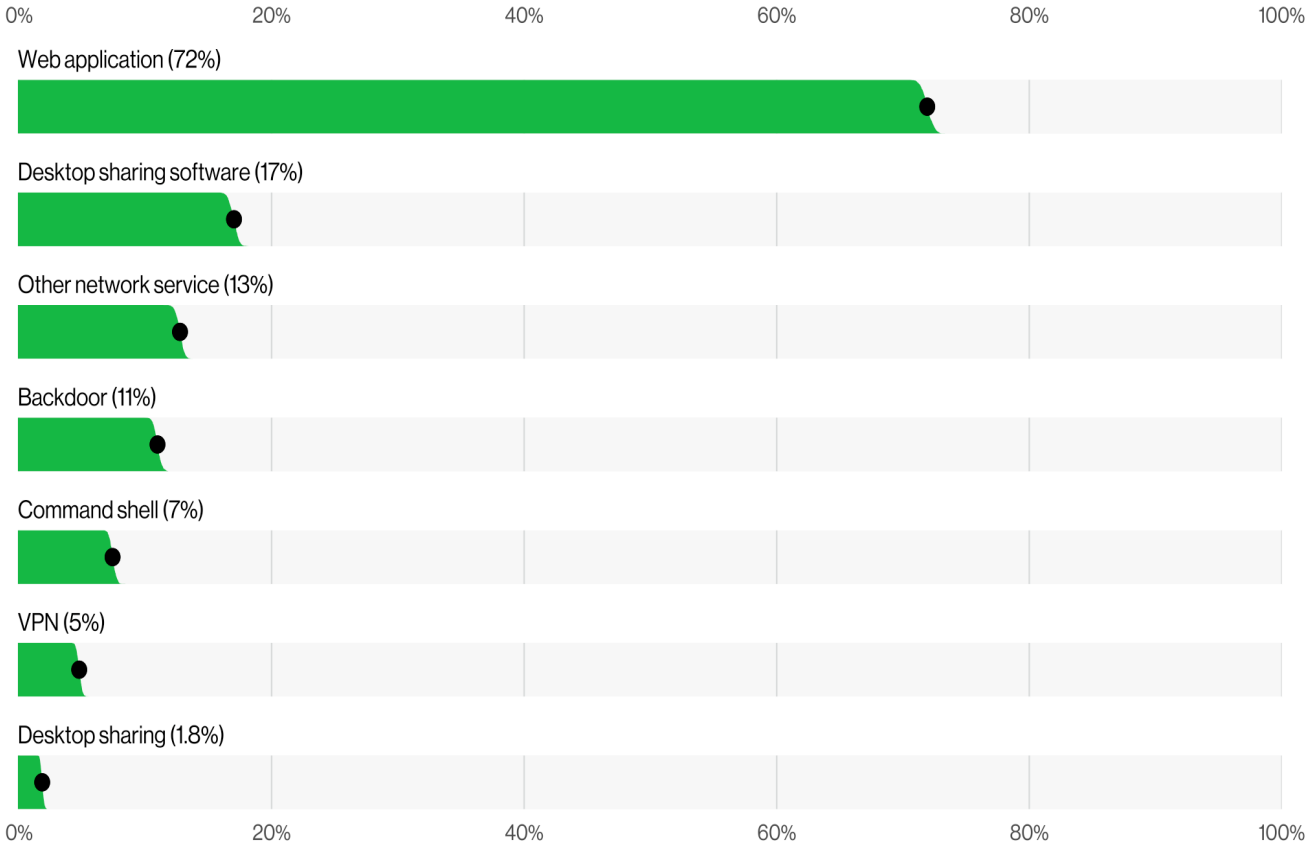


Figure 1. Known 'initial access vectors' over time in non-Error, non-Misuse breaches (n in 2025 dataset=9,891)

- Three main ways that organizations are compromised, Credential abuse, Phishing and Exploitation of vulnerabilities
- Credential abuse shows up in over 30% of all breaches in our dataset (dating back to 2018) and 21% for this year's report
- 34% of the breaches involve credentials getting compromised, sometimes as a means of the attack and other times as an outcome

Top Vectors Associated with Stolen cred



- Web applications (72%), which includes things like email servers, and VPN (5%) represent some of the common initial access
- Desktop sharing software, such as RDP and remote desktop apps, accounts for 17% of breaches, however these might be associated with initial access or lateral movement.
- Other network services (13%), such as internal management services used within an organization, along with backdoor and command shell, represents internal lateral movement, accounting for 16% of breaches.

Figure 2. Top vectors associated with stolen credentials for the last 5 years of breaches (n =10,784)

Other Actions in Stolen Credentials Breaches

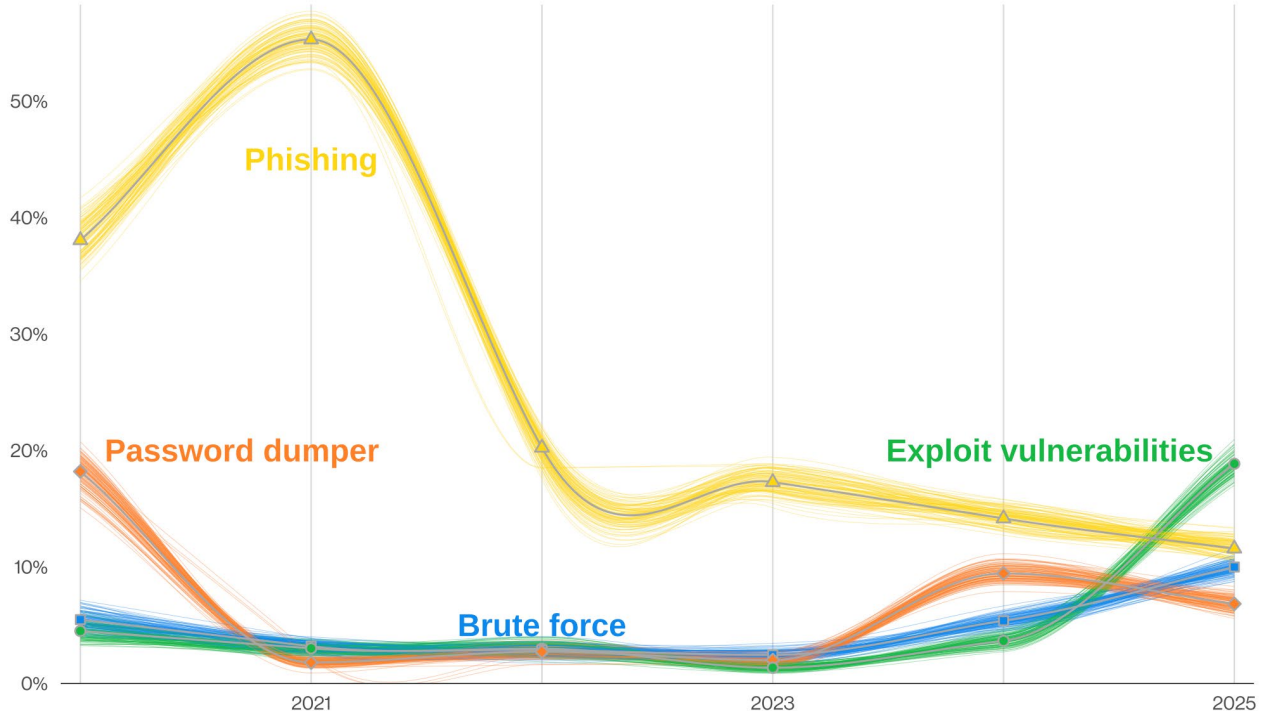
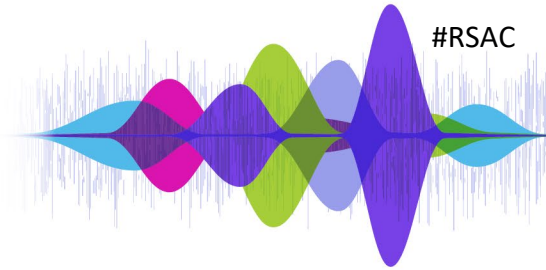


Figure 3. Select action varieties associated with compromised credentials in breaches (n in 2025 dataset=2,211)

- Phishing has historically been the most common tactic associated with compromised credentials, showing up in 26% of the breaches for the last 5 years
- Exploit vulnerabilities, brute force and password dumping has all increased in the last 2 years, and account for (14%) of breaches in the last 5 years
- However, there are about 16% of the breaches involve Unknown actions

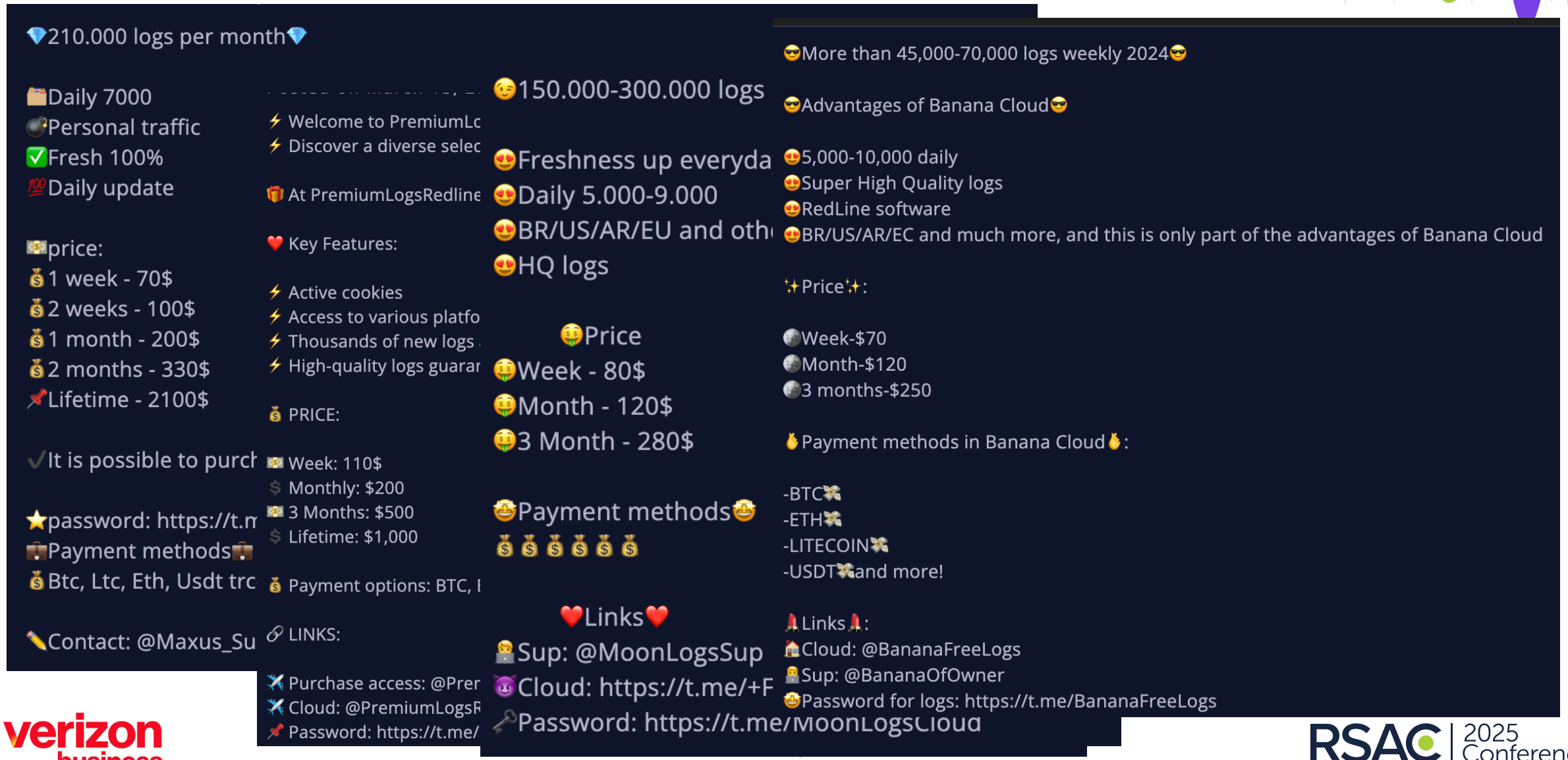
What are Unknowns to the DBIR



- Unknown due to lack of detail from data source
  - Many of the data from the DBIR comes from various data sources and some capture different levels of details
  - Example: “We know malware was used, but we didn’t report what type”
- Unknown due to lack of information
  - In some events, a root cause cannot to be determined due to lack of logs or other investigative limitations
  - Example: “Unable to determine the source of infection due to login logs only being retained for 30 days”

So why so many “Unknowns” in our credential breaches?

Logs, Logs and more Logs



RSAC 2025 Conference

Infostealer Ecosystem

Commodity

Infostealer Malware

- Infostealers largely operate as a Malware as a Service model (MaaS)
- The main players are
  - Redline
  - RisePro
  - Lumma Stealer
  - Vidar
- Distribution
  - Search Engine Optimization (SEO) Poisoning and Malvertising
  - Social Media
  - Other Malware
  - Email

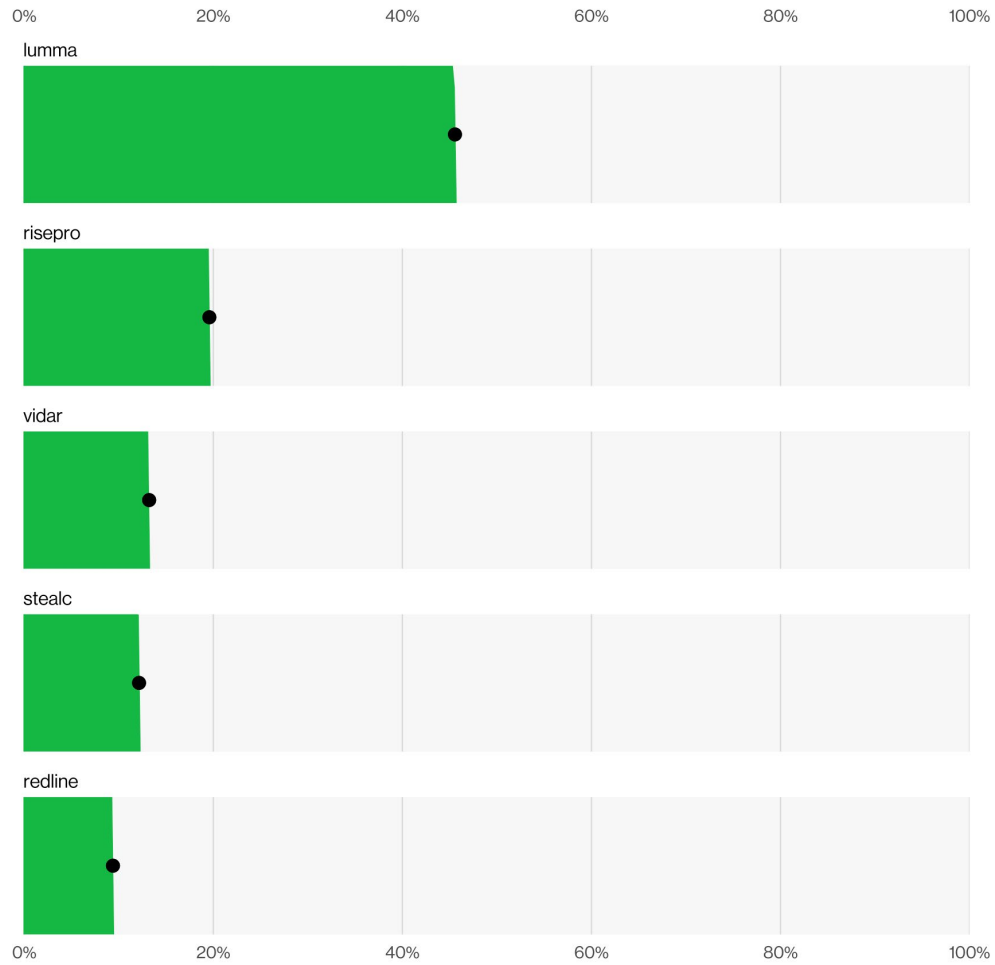
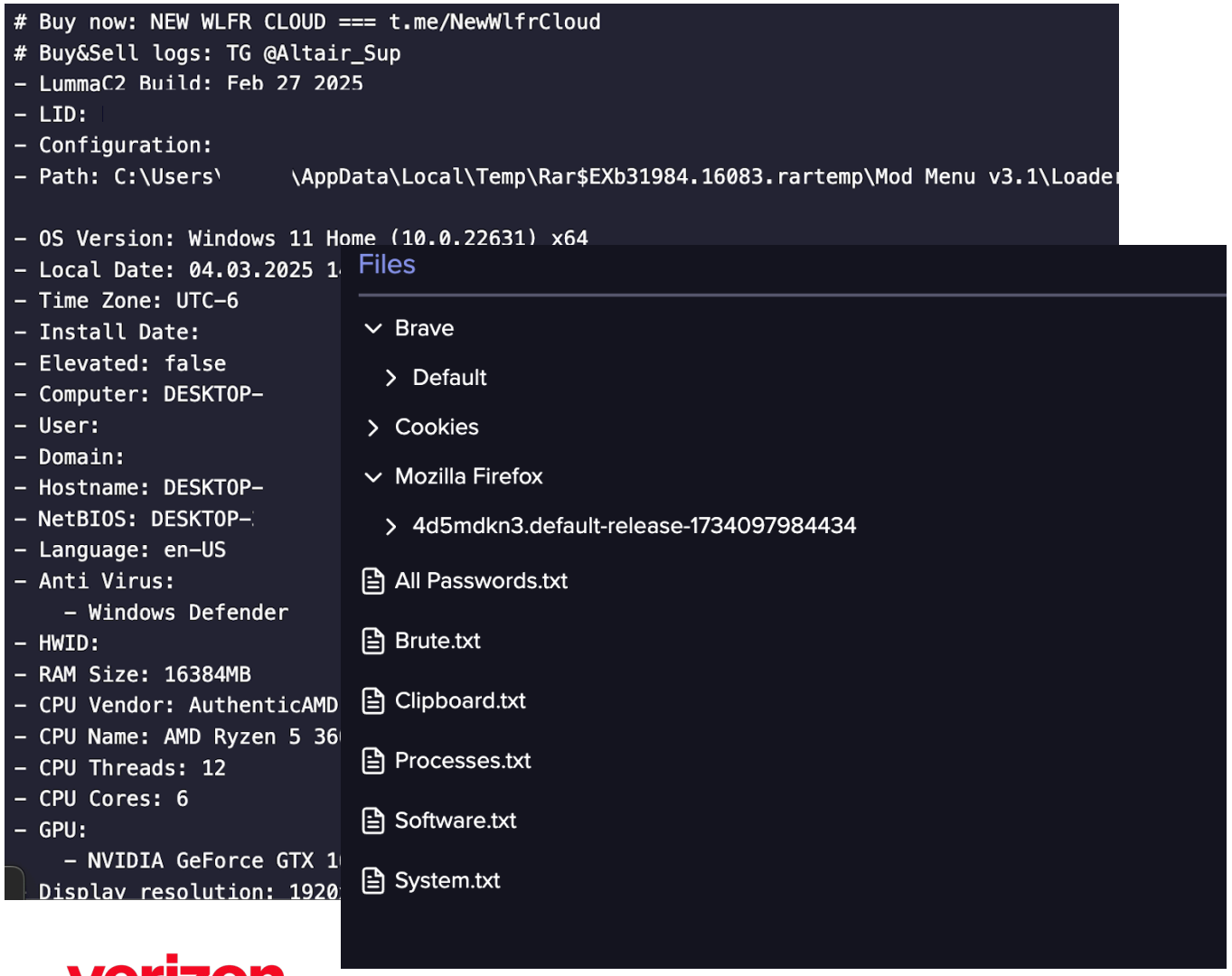


Figure 4. Percentage of infostealer logs posted on criminal marketplaces in 2024 (n=7,339,855)

Infostealer Log



- Saved passwords
- Stored Cookies
- ”Interesting files”
  - Telegram chats
  - Desktop files
  - Remote support software
- System information
  - Information that would allow an attacker to ”replicate” the victim computer

Infostealer Metrics

- Over 23 million devices were compromised by infostealers in 2024 resulting in 2.1 billion compromised passwords[1]
- Through sampling of infostealer logs, found following:
  - 27 is the median number of unique passwords exposed per infected device
  - 18 is the median number of unique domains per infected device
- About 48% of the passwords are reused for different services, exposing those user accounts to credential stuffing attacks

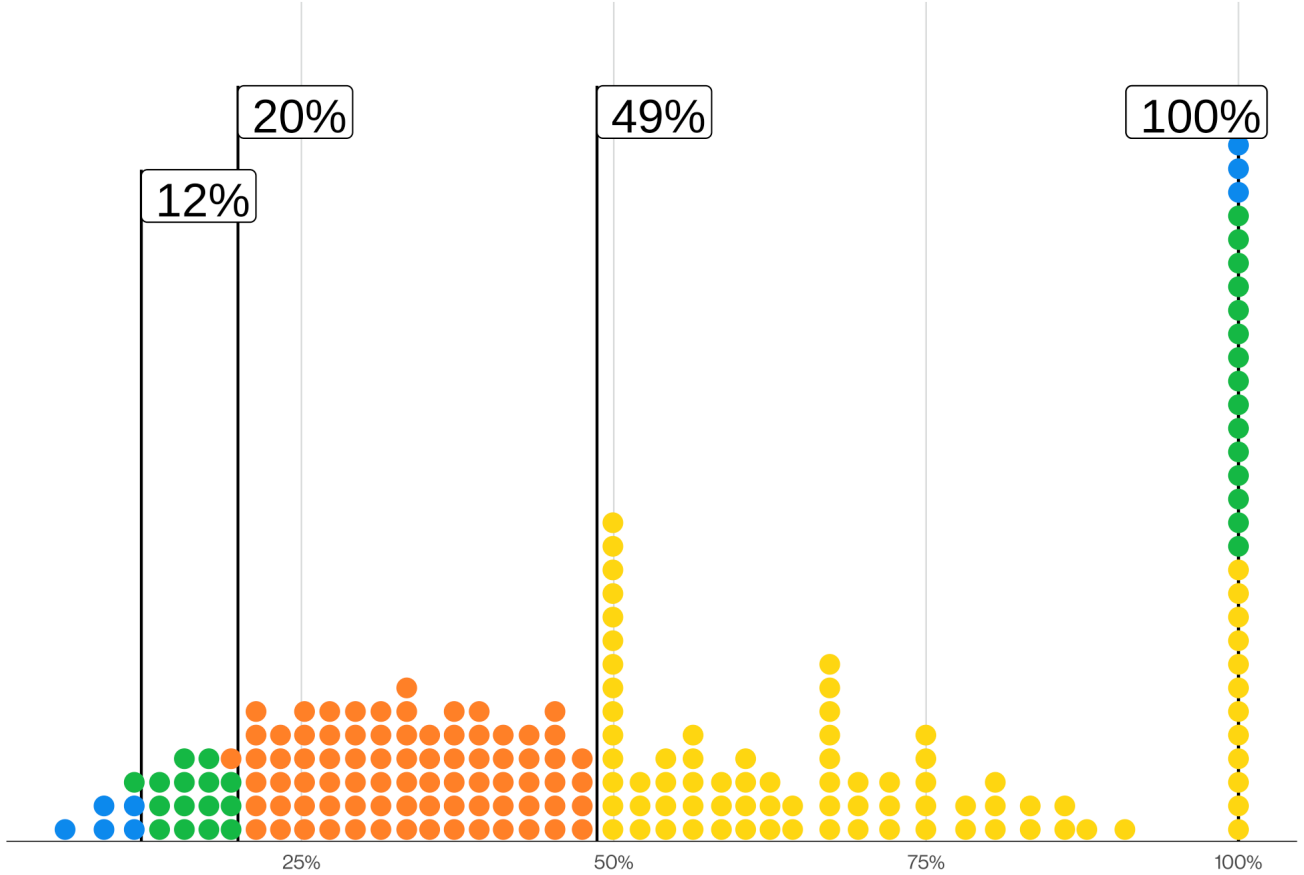


Figure 5. Percentage of unique saved passwords per compromised device found in infostealer logs (n = 2301)

Compromised Credentials

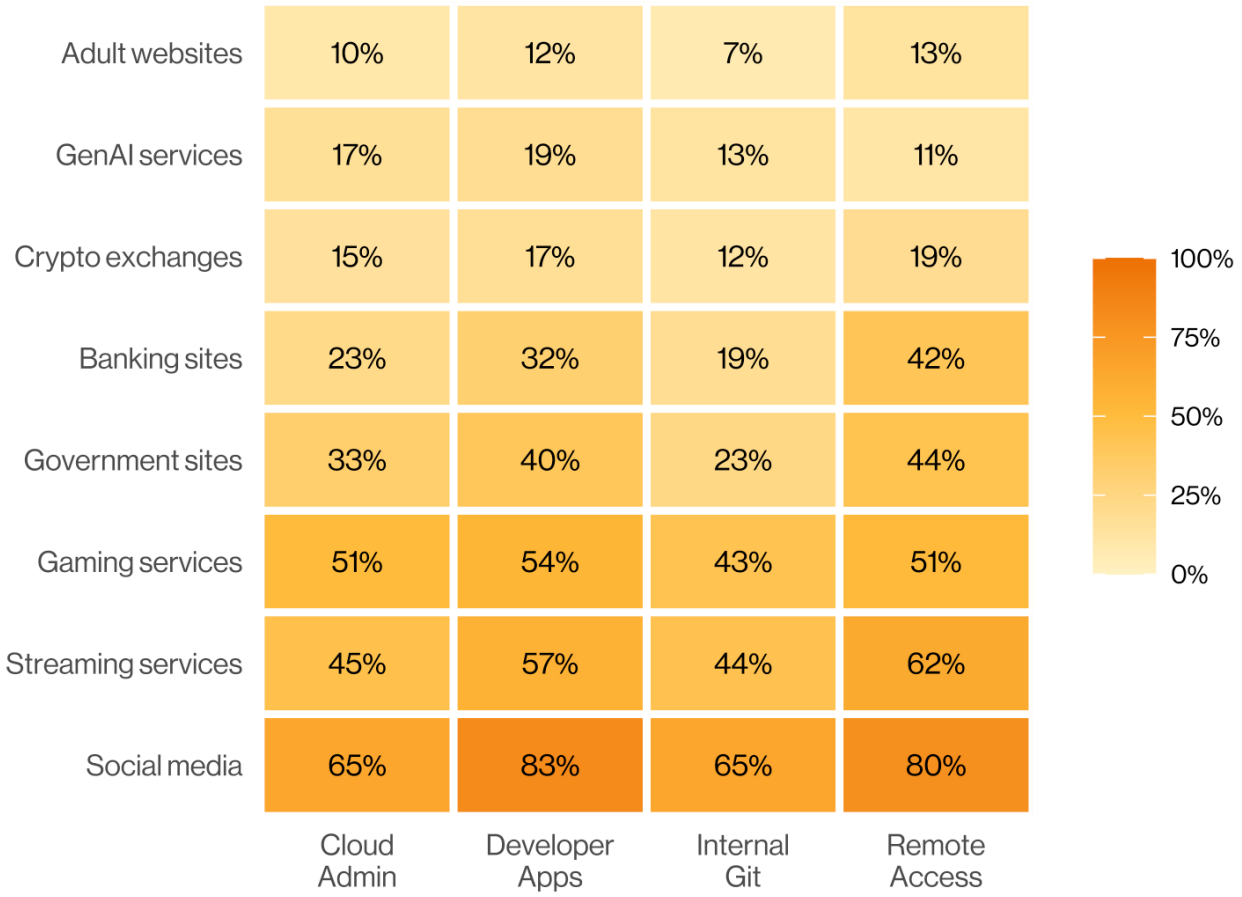


Figure 6. Select types of captured credentials across different infostealer log queries (n=7,855)

- The goal was to determine the overlap that exists between possible corporate resources and personal resources in the infostealer logs
  - **Cloud Administration** – domains associated with managing cloud environments
  - **Developer apps** – domains for second party developer support
  - **Internal Git** – internally hosted git servers
  - **Remote access-** subdomains associated with corporate VPNs endpoints

Bring Your Own ~~Infection~~ Device

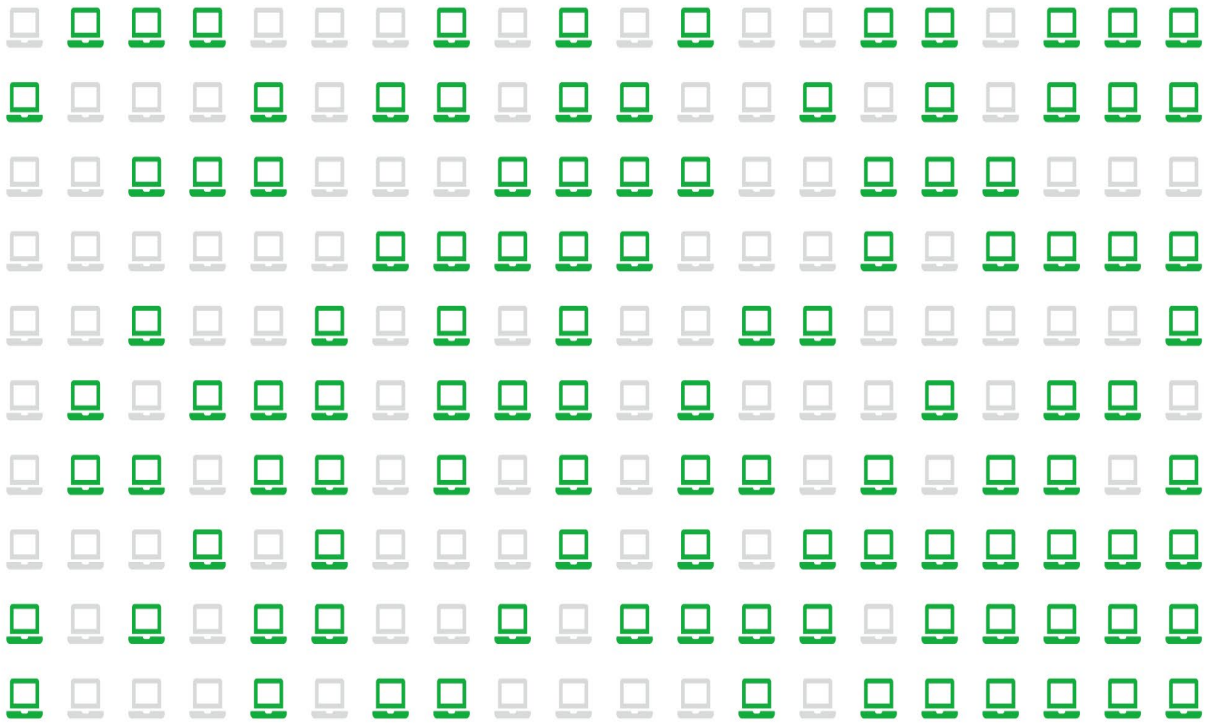


Figure 7. Percentage of non-managed devices with corporate logins in infostealer logs (each glyph is 0.5%)

- Analysis on infostealer credential logs in 2024 revealed that 30% of the compromised systems can be identified as enterprise licensed devices
- However, in our samples, 46% of the systems that had corporate logins in their compromised data were non-managed, and were hosting both personal and business credentials
- These are most likely attributable to a BYOD program or are otherwise being used outside of permissible policy
- Having these devices outside of the organizations control hinders the ability of the organization to even know that these credentials were compromised

RSAC 2025 Conference

Infostealer Ecosystem

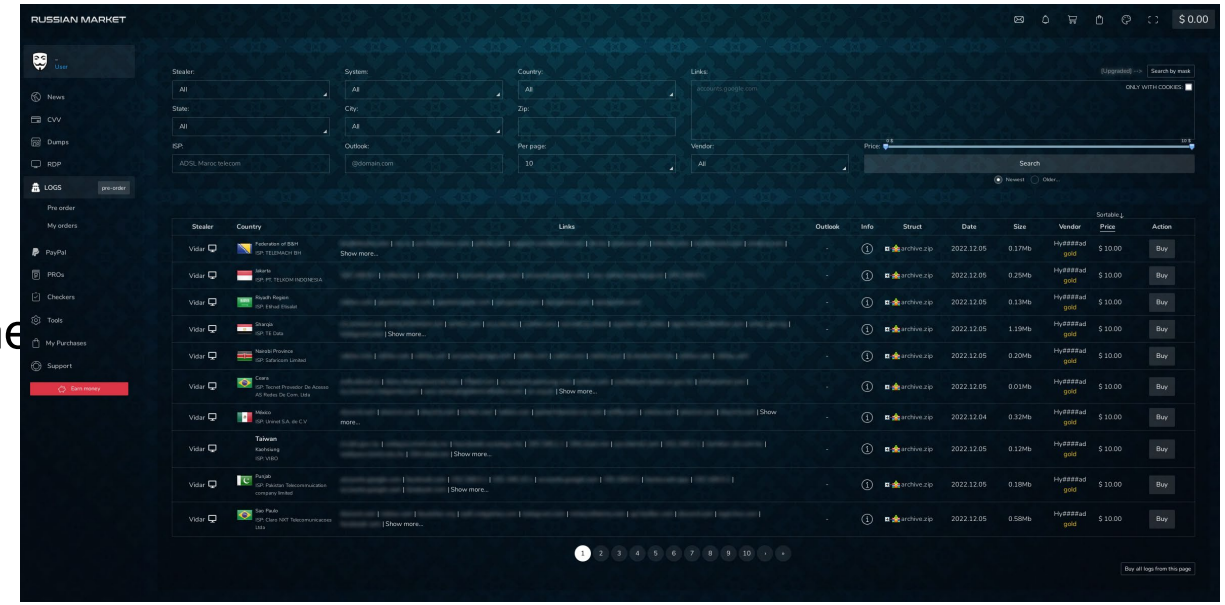
Marketplaces

Many Voices.
One Community.

Credential Markets

- Genesis Market
  - Specialized in selling “bots”
  - Bots had access to access to active cookies and could be used to proxy connections
  - Shut down by law enforcement April 2023- Operation Cookie Monster
  - Allegedly 80 million credentials and 1.5 million compromised systems[5]
  - Costs between $1 to $170[3]
- Russian Market
  - Sells raw infostealer logs
  - Robust search engine to search through the available credentials associated with domains in the logs
  - Each log is typically priced at $10[3]

THIS WEBSITE HAS BEEN SEIZED
OPERATION COOKIE MONSTER
Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.
Been active on Genesis Market? In contact with Genesis Market administrators? Email us, we're interested: FBIMW-Genesis@fbi.gov
FBI
AFP
NCA
EUROPOL
EUROJUST
POLIISI
POLITIE
GUARDIA CIVIL
Polisen



Telegram Channels

- Live Logs
  - Logs collected from malware campaigns are directly posted to the channel
  - Gives buyers quick access to the logs which increases likelihood that cookies and credentials are still valid
- Private channels
  - Invite ($$) only
  - Logs are posted to the channel as they become available
  - First come, first serve
- Sample logs
  - Advertising
  - Small number of logs posted across different channels

Market Analysis

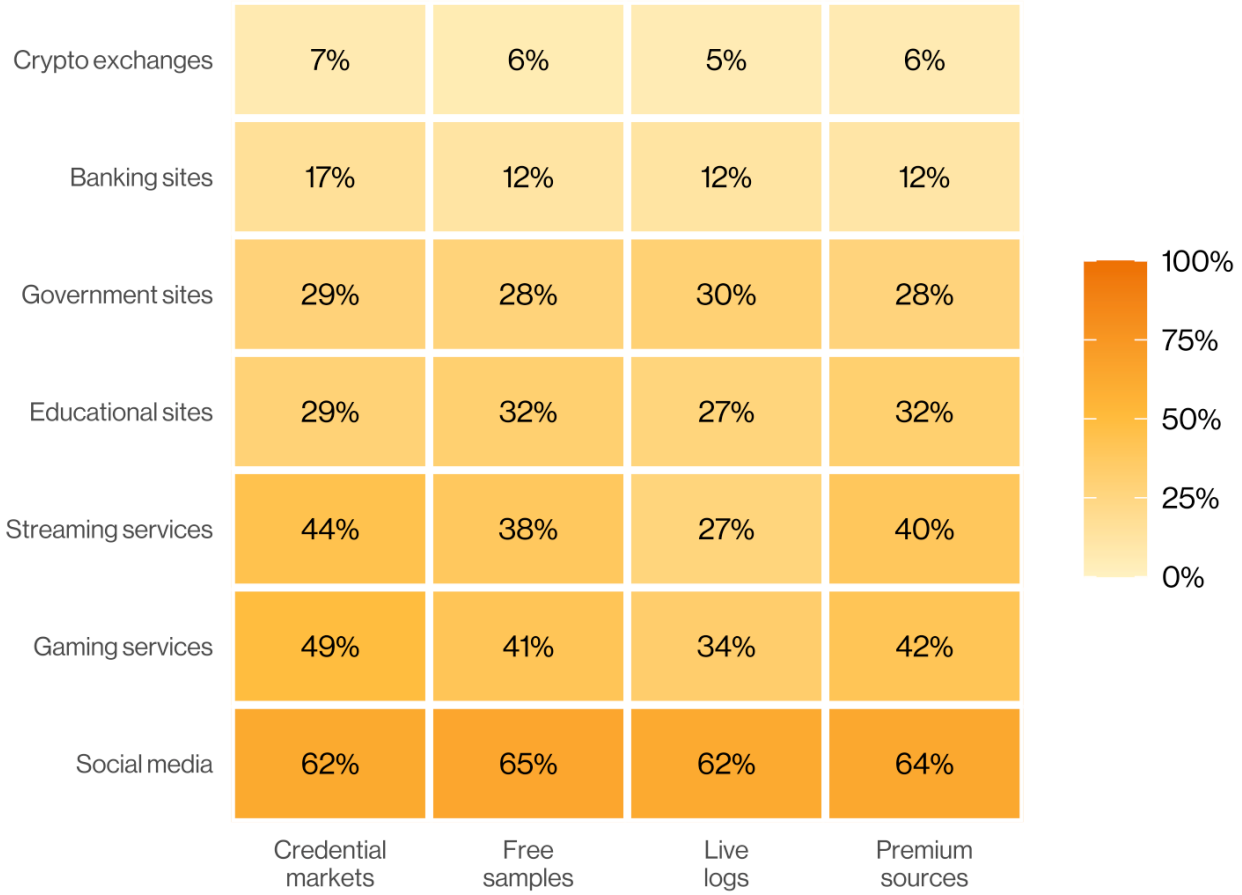


Figure 8. Select types of captured website credentials across different infostealer log sources (n=33,933)

- Based on samples pulled from each of the different sources, there's a lot of similarity in the types of domains that show up
- Social media shows up consistently across all the samples, with over 60% having at least one set of social media credentials
- "High value" targets like banking + crypto accounts show up across the samples, even in the free offerings
- If the type of credentials aren't the differentiator, then perhaps the "freshness" and quantity of the logs are the more important for the buyers

RSAC 2025 Conference

Infostealer Ecosystem

Buyers

Many Voices.
One Community.

Account Take Overs – Cookie Hijack

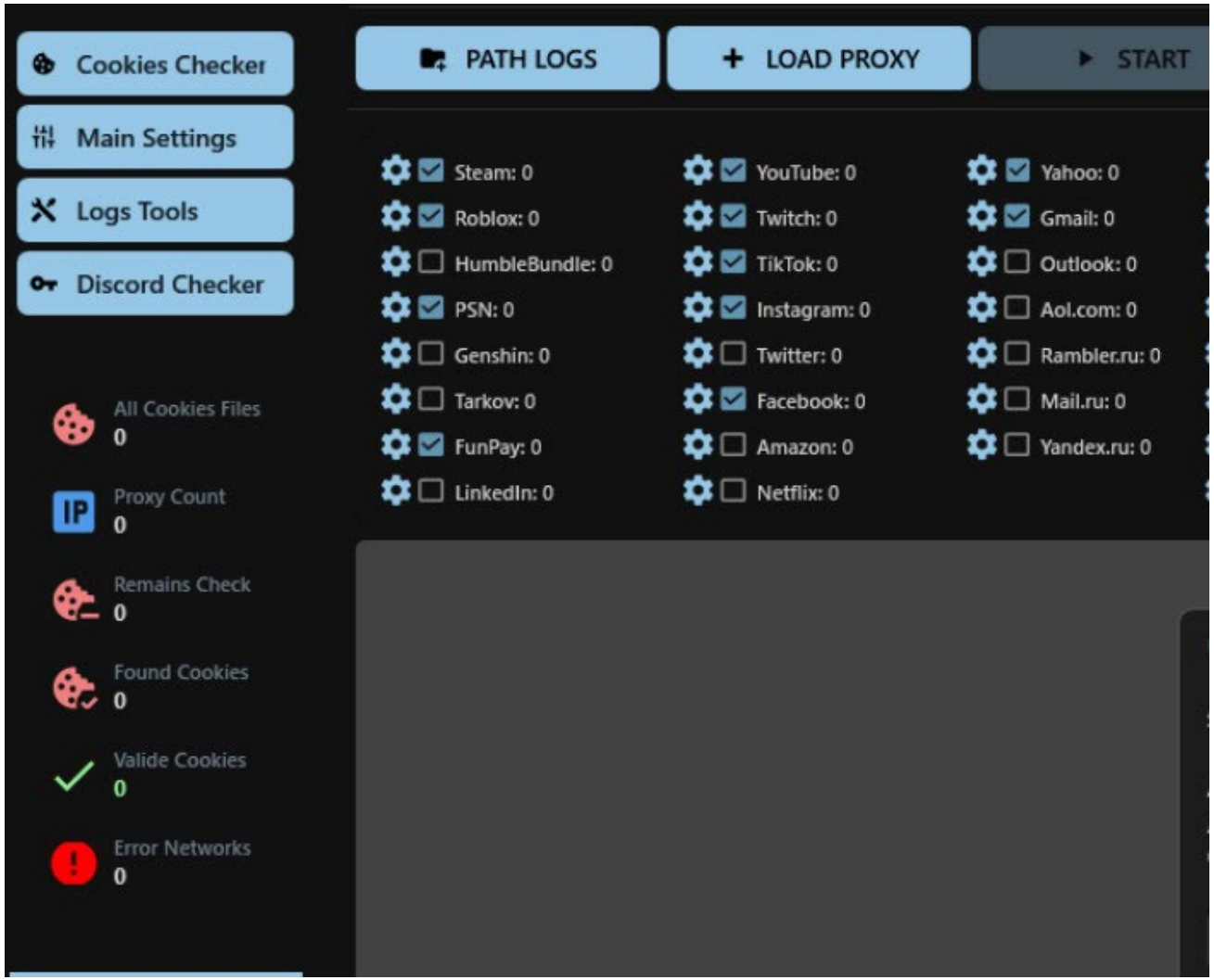
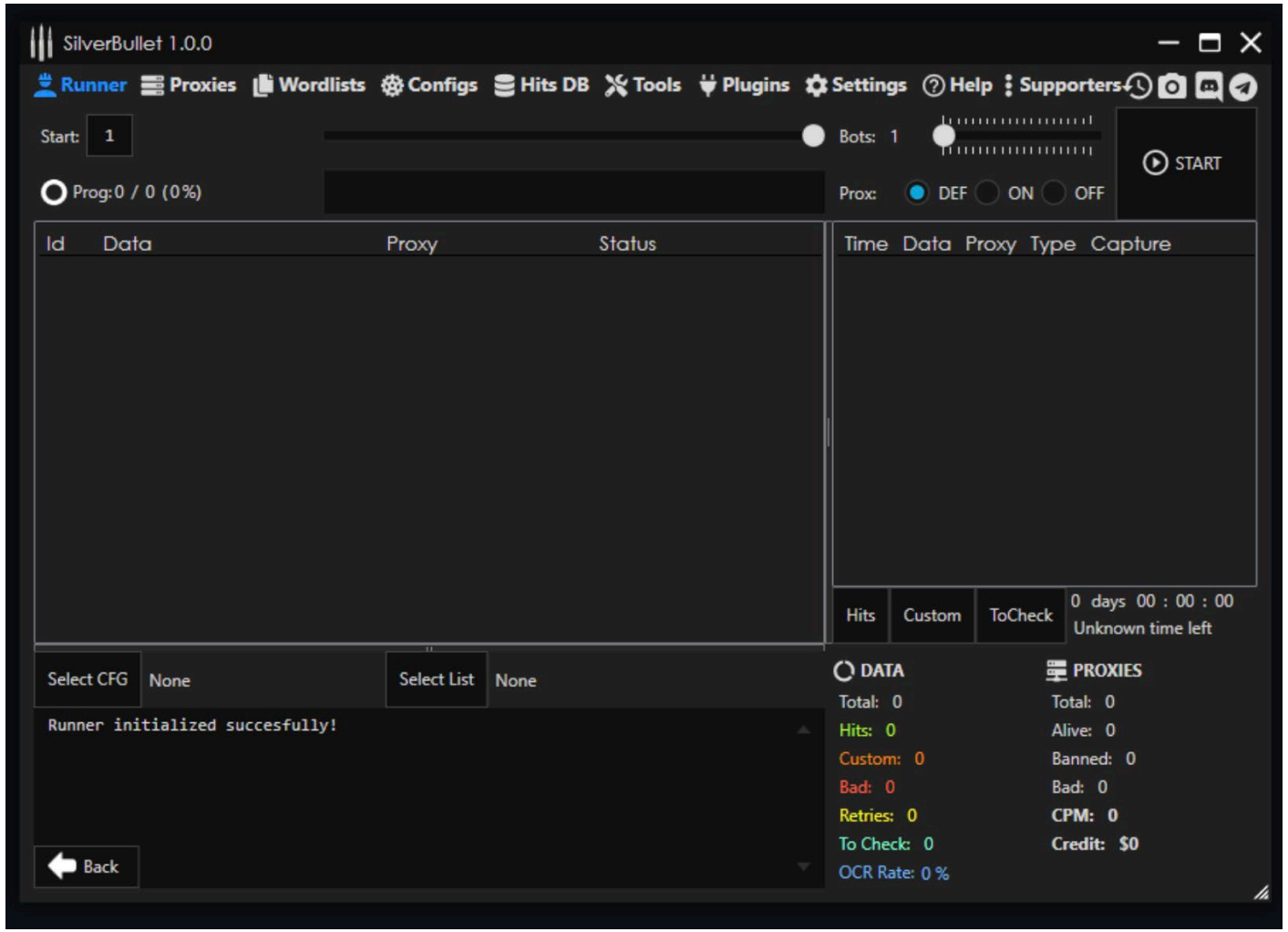


Image of example cookie checker[4]

- Attackers just need a collection of infostealer logs, proxies and a tool to that can check cookies
- The cookie checkers gather session cookies and replay them against the server to verify if the cookies are still valid
- These session cookies can sometimes be used to bypass MFA
- Accounts can then be updated with new passwords and emails

Account Take Overs - Credential Stuffing



- Instead of using the cookies, which often have expirations, attackers will leverage stolen passwords to create large lists of passwords and usernames to target other services
  - This means, not just the services that directly collected by the infostealer are risk, but any service which the user may have reused the password
- Collections of known good usernames and passwords are sold and shared as “Combo lists”
- Various accessible and free credential stuffers
  - Most of these tools can leverage proxy to help hide the source of the attack
  - Services can be targeted by purchasing ”Configs” which describe the URL end point and headers used for the attack

Account Take Overs - Credential Stuffing pt.2

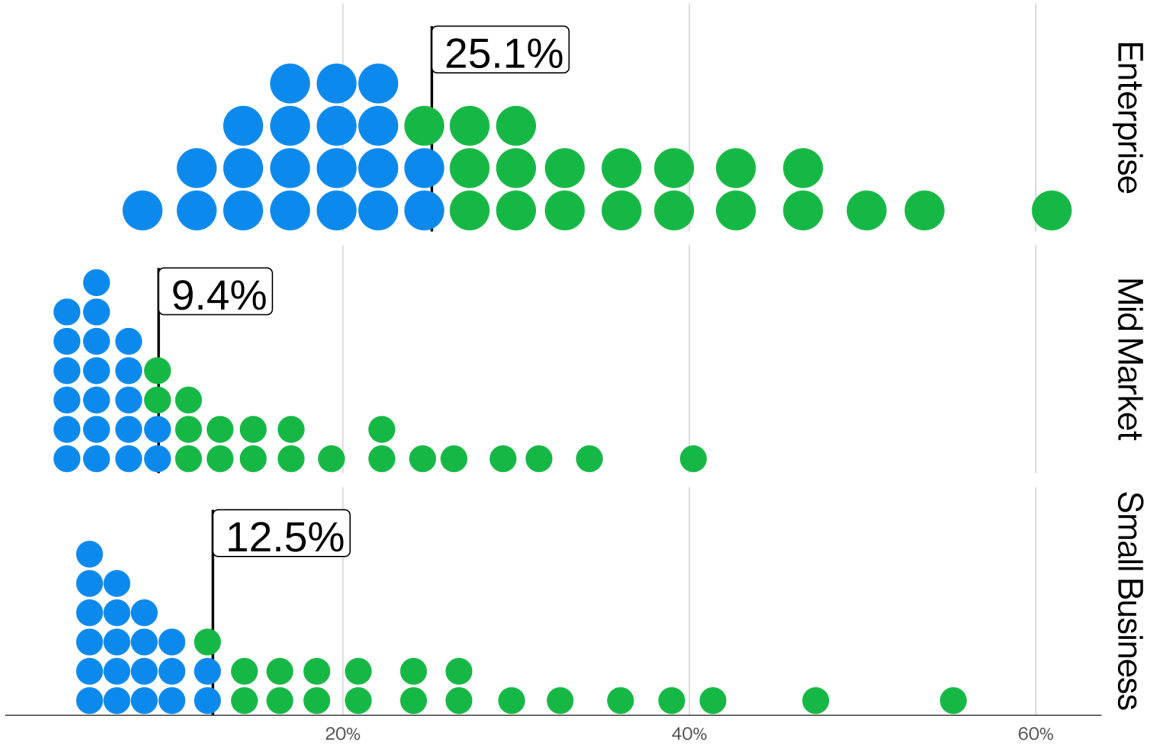


Figure 9. Credential stuffing as a percentage of daily authentication activity

- By looking at authentication logs for SSO provider, we find that the median daily amount of credential stuffing attacks as authentication attempts is 19%
  - 25% for Enterprise
  - 9.4% for Mid market
  - 12.5% for Small businesses
- The highest percentage of credential stuffing we found for one day was 46%
- These attacks target two major vulnerabilities:
  - Users' reuse of passwords
  - Lack of multi-factor authentication

Initial Access Brokers (IAB)

- Threat actors who specialize in getting initial access and reselling that access to a third party
- IABs will often post the access they have on forums with information on the type of access, the rights associate with the access and the industry of the victim
- Access can be in the form of webshells, bot access, and valid compromised VPN or RDP accounts
- RDP is by one of the most common type of access provided, followed by VPN

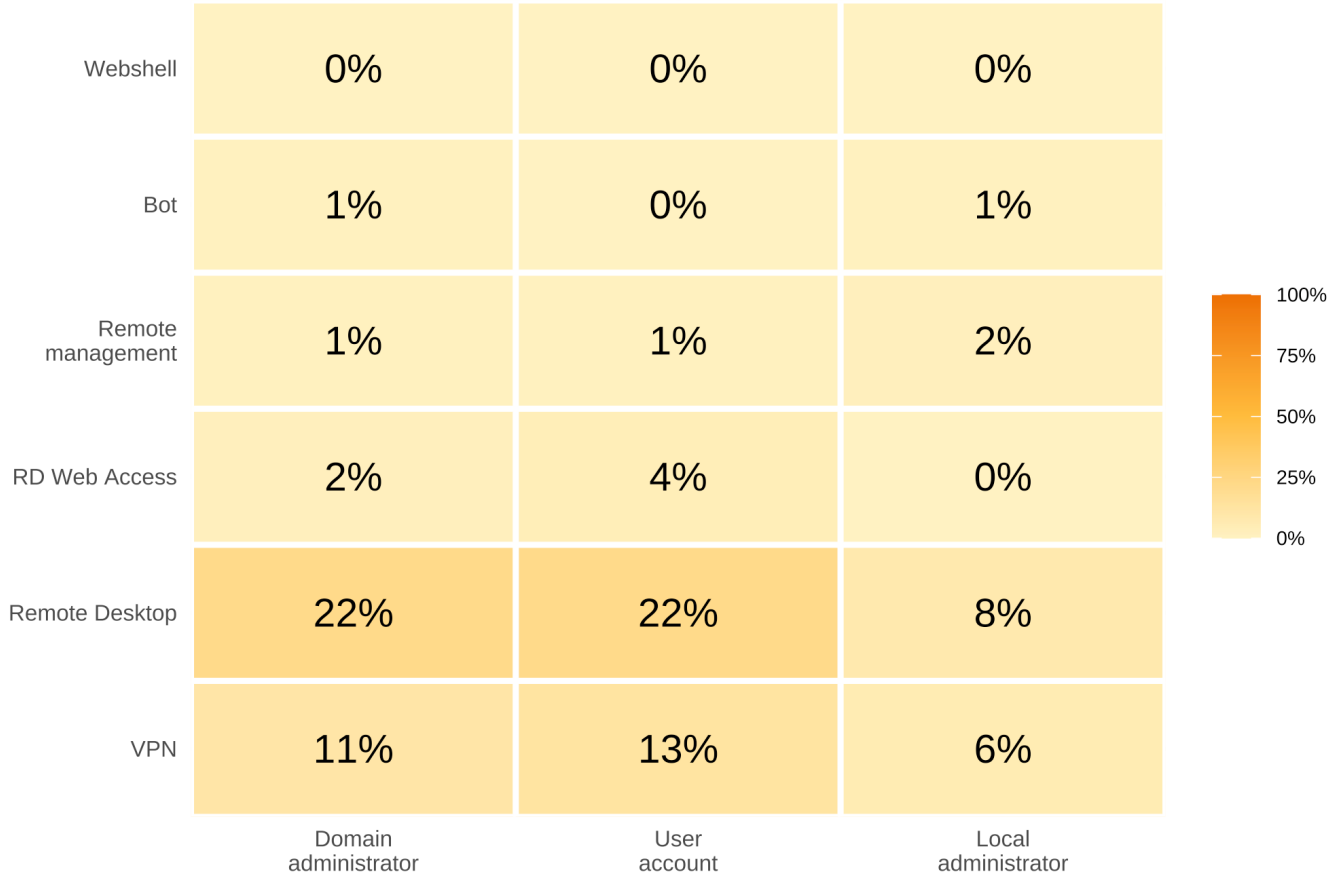


Figure 10. Access types and privileges posted to initial access broker forums (n=260)

Stolen Creds and Ransomware

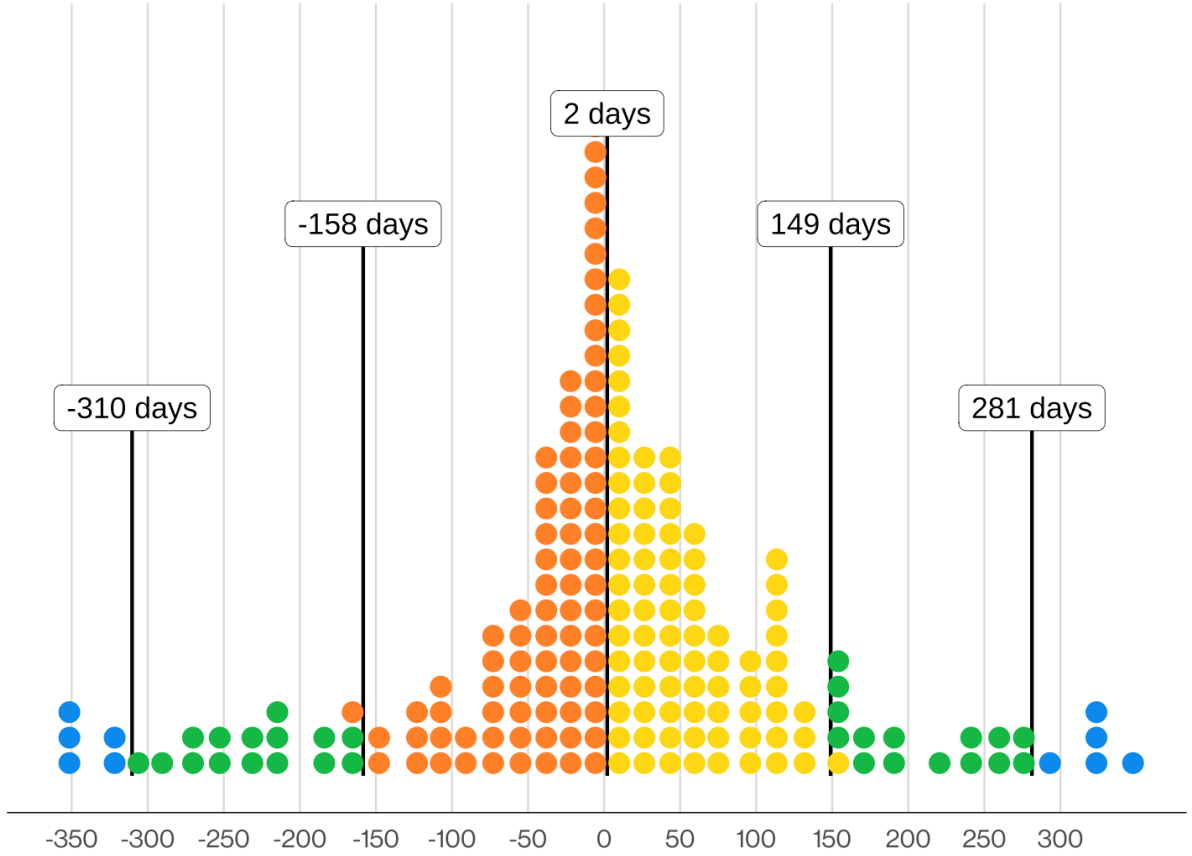
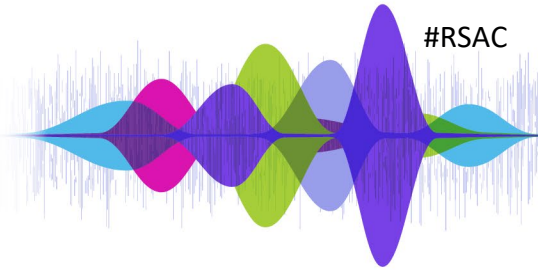


Figure 11. Difference in days between ransomware posting and infostealer log discovery (n=503 – each dot is 2.52 ransomware victims)

- By correlating infostealer logs and marketplace postings with the internet domains of victims that were disclosed by ransomware actors in 2024:
  - 54% of those victims had their domain show up in the credential dumps (for instance, as a URL the credentials allegedly gave access to) and
  - 40% of the victims had corporate email addresses as part of the compromised credentials.
- This suggests these credentials could have been leveraged for those ransomware breaches, pointing to potential access broker involvement as a source of initial access vectors.

Apply What I Have Learned Today



- Next week you should:
  - Review authentication requirements for core infrastructure
  - Ensure MFA is required for authentication
- In the first three months following this presentation you should:
  - Review your inventory of authentication and authorization systems
  - Inventory authentication requirements for key platforms and services
  - Conduct a table top exercise to determine process for resolving an notification of corporate account showing up in an infostealer log
- Within six months you should:
  - Review with product teams risk associated with account take overs of customer accounts and different types of internal employees (developers, HR, executives, etc.)

RSAC 2025 Conference

Many Voices.
One Community.

Questions?

DBIR: verizon.com/dbir
Email: dbir@verizon.com

If you are interested in becoming a contributor to the annual Verizon DBIR (and we hope you are), the process is very easy and straightforward.
Please email us at dbircontributor@verizon.com.

Citations and Resources

1. Flashpoint 2025 Global Threat Intelligence Report: https://www.flashpoint.io/resources/report/2024-global-threat-intelligence-report/
2. https://www.secureworks.com/research/the-growing-threat-from-infostealers
3. https://flare.io/learn/resources/the-stealer-malware-ecosystem-research-report/
4. https://flare.io/learn/resources/blog/infostealer-malware/
5. https://www.justice.gov/archives/opa/pr/criminal-marketplace-disrupted-international-cyber-operation

RSAC™ 2025 Conference

Many Voices.
One Community.